NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

(North Dakota) North Dakota regulators say 21,000-gallon saltwater spill contained at Divide County oil well. The North Dakota Oil and Gas Division reported February 17 that 500 barrels of saltwater were contained and recovered on site, following a 21,000-gallon spill of saltwater at a Murex Petroleum Corp. oil well in Divide County February 15. Officials reported that a pump leak was the cause of the spill.
http://www.dailyjournal.net/view/story/d3cdd485703a4e52bb7ae2dccfa26285/ND--Divide-County-Spill/

(North Dakota) About 1,300 gallons of oil spill in northwest North Dakota; cleanup is underway. The North Dakota Department of Health reported February 17 that approximately 1,300 gallons of oil spilled in Cartwright when a semi-truck that was being filled with fresh water at Caliber Midstream Water Depot spilled residual oil through the truck's overflow vent. Officials reported that cleanup was underway.
http://www.dailyjournal.net/view/story/3771f00fa03a4f0a839b094acfa5fb8a/ND--Oil-Spill-McKenzie-County/

(North Dakota) Drug explosion follows oil boom on North Dakota Indian reservation. Local and federal officials estimate 90% of the drugs on the MHA Nation reservation now come from other states or countries.
http://www.latimes.com/nation/la-na-ff-north-dakota-meth-20150222-story.html#page=1

Regional

(Idaho) Shoshone County sheriff's deputies searching for escaped inmate. Authorities are searching for a potentially armed and dangerous inmate who escaped from the Shoshone County Jail in Idaho February 17. Deputies are investigating how the inmate managed to escape from the jail.
http://www.khq.com/story/28134115/shoshone-county-sheriffs-deputies-searching-for-escaped-inmate

(Minnesota) Mpls. firefighters battle cold at steel plant fire. Investigators announced that a spark from a cutting tool being used too close to combustible

aluminum shavings was the cause of a 3-alarm fire February 18 at Alliance Steel in Minneapolis, and frigid temperatures coupled with the location of the fire made it difficult for firefighters to contain the blaze. http://www.kare11.com/story/news/2015/02/18/mpls-firefighters-battle-cold-at-steel-plant-fire/23603833/

National

(National) AP Exclusive: Fuel-hauling trains could derail at 10 a year. The federal government predicts that trains hauling crude oil or ethanol will derail an average of 10 times a year over the next two decades, causing more than $4 billion in damage and possibly killing hundreds of people if an accident happens in a densely populated part of the U.S. http://abcnews.go.com/US/wireStory/ap-exclusive-fuel-hauling-trains-derail-10-year-29139529

(National) Bitter cold causes cracked rails, more major delays on Metro, Amtrak, VRE. Virginia Express commuter trains, Metro, and Amtrak trains running along the Northeast corridor including Virginia and Washington, D.C., were delayed or forced to run on a reduced schedule February 20 after cracked rails and switch issues that were triggered by cold temperatures. http://www.wjla.com/articles/2015/02/another-day-of-extremely-cold-weather-causes-metro-amtrak-delays-111622.html

(National) NSA planted surveillance software on hard drives, report says. The National Security Agency is able to infect hard drives with surveillance software to spy on computers, Reuters said on Tuesday, citing information from cyber researchers and former NSA operatives. http://www.cnet.com/news/nsa-planted-surveillance-software-on-hard-drives-report/

International

(International) Somalia extremists urge attacks on US shopping malls. A video purported to be by Somalia's al-Qaida-linked rebel group al-Shabab urged Muslims to attack shopping malls in the U.S., Canada, Britain and other Western countries. U.S. authorities said there was "no credible" evidence suggesting a U.S. mall attack was in the works. http://www.cnbc.com/id/102446111

(International) Ongoing cyber attack on banks worldwide creates billion dollar loss. Kaspersky security researchers discovered that cyber criminals robbed over 100 financial institutions worldwide of up to $1 billion by using spear-phishing attacks exploiting 2 vulnerabilities in Microsoft Office and 1 vulnerability in Microsoft Word to install malware and infiltrate institutions' networks. The attackers cashed in by instructing ATMs to dispense money at specific times without payment cards, opening accounts with fake balances, and artificially inflating account balances of bank customers and then transferring the surplus to their accounts in China and the U.S. http://news.softpedia.com/news/Ongoing-Cyber-Attack-on-Banks-Worldwide-Creates-Billion-Dollar-Loss-473391.shtml

(International) Firmware of over a dozen hard drive brands altered to lodge malware. Kaspersky researchers discovered that a cyber-espionage group calling itself Equation modified hard drive firmware in over 12 brands to potentially infect tens of thousands of computers worldwide, including those in sectors such as government and military institutions, nuclear research, oil and gas, telecommunications, transportation, and the financial sector, among others. Reprogramming the firmware allowed attackers to create persistent hidden storage spaces accessible only through specific methods known to them. http://news.softpedia.com/news/Firmware-Of-Over-a-Dozen-Hard-Drive-Brands-Altered-to-Lodge-Malware-473365.shtml

(International) Arabic threat group attacking thousands of victims globally. Kaspersky Lab security researchers reported that "Desert Falcons," the first known full-scale Arabic cyber-espionage group, has used spear-phishing and social engineering techniques to deliver two backdoors though 100 malware samples to infect Windows PCs and Android devices of targets based in Egypt, Palestine, Israel, Jordan, the U.S., and other countries for at least 2 years. The malware has full-backdoor capability as well as the capability to steal call and SMS logs in Android versions, and attackers have targeted victims from political, military, government individuals and organizations, media outlets, energy and utility providers, physical security companies, and others holding geopolitical information. http://www.securityweek.com/arabic-threat-group-attacking-thousands-victims-globally

Banking and Finance Industry

(International) Accused Russian hacker to face charges in US court. A Russian national was extradited to the U.S. and charged February 17 in New Jersey for his alleged involvement in an international scheme that stole more than 160 million credit card numbers resulting in hundreds of millions of dollars in losses to consumers and financial institutions including Dow Jones, 7-Eleven, Nasdaq, Visa, and JetBlue. The suspect, arrested in the Netherlands in 2012, allegedly hacked victims' networks to gain access to usernames and passwords, credit card and personal identifiable information, and sold them to resellers around the world. http://www.msn.com/en-us/news/crime/accused-russian-hacker-to-face-charges-in-us-court/ar-BBhHvhz

(International) Vawtrak trojan downloaded via malicious macro for Microsoft Word. Trend Micro security researchers discovered a new cyber criminal campaign targeting banks including Bank of America, Barclays, Citibank, HSBC, Lloyd's Bank, and J.P. Morgan with emails containing malicious macro-enabling Microsoft Word documents that install the Vawtrak banking trojan by downloading a batch file, a visual basic scripting edition (VBS script), and Powershell file. The malware serves clients modified pages to trick them into providing log in data for Microsoft Outlook, Google Chrome, Mozilla Firefox, and file transfer protocol (FTP) clients. http://news.softpedia.com/news/Vawtrak-Trojan-Downloaded-Via-Malicious-Macro-for-Microsoft-Word-473438.shtml

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(South Carolina) Florence police look for Magnolia Mall shooting suspect. One person was wounded when a man opened fire inside the Magnolia Mall in Florence, South Carolina, February 13 following an altercation between two groups of individuals. Police are searching for the gunman and continue to investigate the incident that prompted the evacuation and closure of the mall. http://www.wistv.com/story/28108013/florence-police-evacuate-magnolia-mall

Communications Sector

(West Virginia) Frontier continues to work on damaged cables near train derailment. Frontier Communications technicians continued to work with railroad and public safety officials February 19 to replace fiber-optic cables that were damaged by a train derailment in Fayette County during the week of February 16. A representative reported that broadband service was restored February 18 but voice-service was still down while additional repairs were being made. http://www.wsaz.com/news/headlines/Frontier-Continues-to-Work-on-Damaged-Cables-near-Train-Derailment-292736621.html

Critical Manufacturing

(International) GM recalls over 81K Chevrolet, Pontiac vehicles over power steering problem. General Motors issued a recall for 81,000 model year 2006 and 2007 Chevrolet Malibu, Malibu Maxx, and Pontiac G6 vehicles for issues that could cause power steering to fail. The company reported that the problem has caused one accident but no deaths or injuries. http://www.syracuse.com/news/index.ssf/2015/02/gm_recalls_over_81k_chevrolet.html

(International) Lenovo to stop pre-installing controversial software. Errata Security researchers determined that Superfish adware pre-installed on Lenovo computers hijacks and throws open encrypted connections, allowing hackers to seize connections and listen in through man-in-the-middle (MitM) attacks. Lenovo disabled all Superfish software from its consumer computers and stopped pre-installing the software on its devices, but experts warned that systems could still be vulnerable even after uninstalling the software. http://www.reuters.com/article/2015/02/19/us-lenovo-cybersecurity-idUSKBN0LN0XI20150219

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

Nothing Significant to Report

Energy

(California) Four injured in explosion at Torrance ExxonMobil refinery; air quality alert issued. Four workers were injured following a February 18 explosion at an ExxonMobil oil refinery in Torrance, California, prompting a smoke and ash advisory for the surrounding area. Employees were sent home after the facility was heavily damaged and authorities reported that the blast occurred in a recently installed processing facility. http://www.ocregister.com/articles/refinery-651559-explosion-torrance.html

Food and Agriculture

(International) Bird flu strikes second California poultry farm. The U.S. Department of Agriculture (USDA) confirmed February 13 the presence of the Eurasian H5N8 virus at an 114,000-bird chicken farm in Kings County, prompting Canadian authorities to issue a ban on poultry raised, processed, or shipped from California. The outbreak reportedly began February 2 with an increased mortality among chickens, and was confirmed February 12 when the premises were also quarantined. http://www.capitalpress.com/California/20150216/bird-flu-strikes-second-california-poultry-farm

Government Sector (including Schools and Universities)

(Missouri) City of Columbia website attacked again. An official with the City of Columbia, Missouri, confirmed that the city's official Web site was attacked again February 16 following a February 12 attack that flooded the site with requests from multiple sources, rendering the Web site unavailable. Officials were able to regain control of the site after several hours. http://www.komu.com/news/city-of-columbia-website-attacked-again/

(Nevada) School canceled in Winnemucca after mercury scare. Classes were canceled across schools in the district February 20 after 400 students had their

feet and shoes decontaminated on the football field of Winnemucca Junior High School in Nevada after a student took a salt shaker filled with mercury to the school February 19 leaving trails of it through the hallways and on the school bus. Three other schools in the area were placed under a precautionary lockdown to ensure the mercury did not travel to other schools. http://www.rgj.com/story/news/2015/02/19/mercury-spill-prompts-lockdown-winnemucca-school/23701433/

Information Technology and Telecommunications

(International) Commercial spyware found in enterprise environment. Security researchers at Lacoon Mobile Security and Check Point discovered 18 different commercial remote access trojan (mRAT) spying tools that connect to the company's Wi Fi and communicate with the command and control (C&C) server on 1,000 of 900,000 corporate mobile devices tested. The spyware, generally marketed for monitoring children, allows employers to track the location of users, log activity on the device, access emails, texts, and contacts, and possibly activate the device's microphone for recording. http://news.softpedia.com/news/Commercial-Spyware-Found-in-Enterprise-Environment-473785.shtml

(International) Android malware takes over device's shutdown process. AVG security researchers discovered a new mobile malware strain affecting Android devices that hijacks the shutdown process and obtains root permission to run nefarious activities such as initiating calls or taking pictures while the phone appears to be off. http://news.softpedia.com/news/Android-Malware-Takes-Over-Device-s-Shutdown-Process-473705.shtml

Public Health

(California) 2 of 7 patients infected die after being exposed to superbug bacteria at UCLA Medical Center. UCLA Ronald Reagan Medical Center in California reported February 18 that 179 patients may have been exposed to the carbapenem-resistant enterobacteriaceae after at least 2 patients died and 5 others were infected following exposure to the drug-resistant superbug bacteria between October 2014 and January. Hospital officials stated that the potential exposure occurred during complex endoscopic procedures and that the two

infected scopes were removed while the hospital undergoes deep decontamination. http://losangeles.cbslocal.com/2015/02/18/2-patients-die-7-infected-after-being-exposed-to-deadly-superbug-bacteria-at-ucla-medical-center/

Transportation

(Virginia) Flights diverted from Dulles after pipe bursts. Normal operations were restored at Dulles International Airport in Virginia after a water pipe that burst in the airport's control tower triggered an alarm and prompted an evacuation. About 17 flights were cancelled, 13 additional flights were delayed, and an unspecified number of flights were diverted to other airports while the scene was cleared. http://washington.cbslocal.com/2015/02/16/flights-diverted-from-dulles-after-pipe-bursts/

Water and Dams

(West Virginia) Water system to restart; WVAW issues precautionary boil water advisory. West Virginia American Water issued a precautionary boil water advisory for approximately 2,000 customers served by the company's Montgomery water system while the treatment plant is brought back online after it was shut down as a precaution following the derailment of a train hauling crude oil February 16 along a tributary of the Kanawha River near the plant. The decision to restart the water treatment plant was made after three rounds of water quality testing at the water treatment plant and at various locations in the river showed non-detectable levels of the components of crude oil. http://www.montgomery-herald.com/news/water-system-to-restart-wvaw-issues-precautionary-boil-water-advisory/article_f9f6f756-b6d3-11e4-9bd5-3f8ae77c3f7b.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165